IMPLEMENTASI SISTEM KRIPTOGRAFI DENGAN ALGORITMA BLOWFISH UNTUK MENGAMANAKAN DATABASE PADA MINIMARKET HAPPYMART

Mauliga Penyejuknate[1], Sejati Waluyo[2],Ika Susanti[3], Dani Anggoro[4]
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
e-mail: [1]Mauliga34@gmail.com, [2]sejati.waluyo@budiluhur.ac.id, [3]ika.susanti@budiluhur.ac.id,
[4]dani.anggoro@budiluhur.ac.id

ABSTRAK

Kriptografi adalah ilmu yang mempelajari tentang mensandikan data menggunakan teknologi enkripsi data, merubah suatu data asli kedalam data sandi sehingga informasi yang ada didalamnya tidak dapat dibaca oleh orang yang tidak memiliki kepentingan terhadapa data tersebut. Database sendiri adalah tempat menyimpan dan mengelola data. Pada dasarnya dalam sebuat database, sudah dilengkapi dengan proteksi sehingga tidak semua orng dapat mengakses data tersebut. Akan tetapi orang yang memiliki akses terhadap database dapat dengan mudah mengekplore data tersebut. Sehingga diperlukan sistem proteksi tambahan untuk memproteksi data tersebut baik dari orang dalam maupun orang luar yang berhasil masuk kedalam sistem database. Minimarket HappyMart adalah toko yang melayani kebutuhan masyarakat. Didalam database mereka tersimpan data-data penting berupa data-data penjualan dan barang yang mereka sediakan. Sehingga berpotensi diambil maupun dimanipulasi isi datanya, sehingga membutuhkan proteksi lebih untuk menjaga data mereka. Oleh sebab itu penulis mengembangkan metode sistem kriptografi menggunakan algoritma BlowFish, untuk menyandikan data-data minimarket HappyMart. Sehingga data penjualan dan suplay barang pada minimarket HappyMart dapat terproteksi dari orang yang tidak bertanggung jawab, data yang tersimpan dalam database berupa ciphertext berupa sandi enkripsi sehingga pesan atau informasi dari data yang tersimpan kedalam database tidak bisa dibaca secara langsung diperlukan key atau kunci untuk membuka informasi tersebut.

***Kata Kunci** : Sistem Kriptografi, Database Minimarket, Mensandikan Database*

1. PENDAHULUAN

Keamanan dan kerahasiaan data selalu menjadi masalah dalam suatu organisasi , lembaga pemerintahan, maupun dunia pendidikan. Seringkali sebuah data menjadi sangat berharga dan tidak semua orang diperkenankan untuk mengetahuinya. Namun selalu saja ada pihak-pihak yang ingin berusaha untuk mengetahui isi suatu data dengan cara-cara yang tidak semestinya bahkan bermaksud untuk merusaknya dan mencurinya. Hal ini sering mereka lakukan baik secara online (terhubung ke jaringan) ataupun secara offline (tidak terhubung kedalam jaringan). Apabila terjadi suatu tindakan pembobolan dan pencurian informasi suatu data penting dalam sebuah organisasi, maka akan merugikan pihak yang berkepentingan hal ini dilakukan untuk menjaga agar data yang dianggap rahasia jangan sampai dibaca, diubah, ataupun disebarluaskan oleh pihak yang tidak berkepentingan.karena begitu pentingnya sebuah informasi maka dibutuhkan suatu cara agar informasi tetap terjaga kerahasiannya. Salah satu cara yang digunakan adalah dengan cara menyandikan isi informasi menjadi suatu kode kode yang tidak dimegerti.

Minimarket HappyMart terdapat banyak sekali data-data penting yang merupakan sumber informasi dan asset bagi HappyMart untuk menentukan langkah strategis dalam menjalankan bisnisnya. Data ini tentunya bersifat private, yang artinya hanya orang tertentu saja yang boleh mengetahui data tersebut. Penggunaan sistem database meskipun sudah aman, akan tetapi masih rentan terutama terhadap orang yang memiliki akses terhadap data tersebut. Dimana masih ada kemungkinan data tersebut dimanupulasi atau disebarluaskan kepada orang yang tidak berkepentingan namun dapat memanfaatkan data tersebut. Sehingga perlu adanya poteksi tambahan berupa menyandikan data-data penting tersebut kedalam bentuk sandi sehingga informasi data tersebut meskipun dapat diakses namun tidak dapat dibaca informasi yang ada didalamnya. Oleh sebab itu penulis mengembangkan sebuah sistem pengamanan database menggunakan sistem penyandian kriptografi menggunakan algoritm Blowfish untuk memproteksi data-data penting yang ada di minimarket HappyMart.

Algoritma Blowfish adalah salah satu algoritma yang dapat digunakan untuk melakukan enkripsi data sehingga data asli hanya dapat dibaca oleh seseorang yang memiliki kunci enkripsi tersebut. Algoritma ini menggunakan teknik cipher blok dengan key simetris. Blowfish memiliki ukuran blok 64 bit dan panjang key dari 32 sampai 448 bit. Blowfish menggunakan chipher Feistel dan menggunakan parameter SBOX yang sangat besar dan nilainya bergantung dari key. Strukturnya sangat mirip dengan struktur CAST-128, yang menggunakan SBOX dengan nilai tetap.Algoritma ini menggunakan teknik cipher blok dengan key simetris.

2. LANDASAN TEORI

Kata kriptografi berasal dari bahasa Yunani, “kryptós” yang berarti tersembunyi dan “gráphein” yang berarti tulisan. Kriptografi merupakan ilmu yang mempelajari Teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, antektikasi, integritas dan keabsahan data. Kriptografi juga dapat diartikan sebagai ilmu untuk menjaga kerahasiaan pesan[1].

Blowfish atau disebut juga OpenPGP.Cipher.4 adalah enkripsi yang termasuk dalam golongan Symmetric Cryptosystem. Blowfish merupakana lgoritma kunci simetrik cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneier untuk menggantikan Data Encryption Standard(DES). Metode enkripsi ini diciptakan oleh Bruce Schneier, seorang Cryptanalyst Presiden perusahaan Counterpane Internet Security, Inc pada tahun 1993. Dan dipublikasikan tahun 1994. Blowfish dibuat untuk digunakan pada komputer yang mempunyai mikroprosesor besar (32 bit ke atas dengan cache datayang besar).

Blowfish merupakan cipher blok. Yang berarti selama proses enkripsi dan dekripsi, Blowfish bekerja dengan membagi pesan menjadi blok-blok bit dengan ukuran sama panjang yaitu 64-bit dengan panjang kunci bervariasi yang mengenkripsi data dalam 8 byte blok [9]. Pesan yang bukan merupakan kelipatan 8 byte akan ditambahkan bitbit tambahan (padding) sehingga ukuran untuk tiap blok sama. [2].

Blowfish termasuk dalam enkripsi block Cipher64-bit dangan panjang kunci yang bervariasi antara 32-bit sampai 448-bit.Algoritma Blowfish terdiri atas dua bagian :

1. Key-Expansion Berfungsi merubah kunci (Minimum 32-bit, Maksimum 448-bit) menjadi beberapa array subkunci(subkey) dengan total 4168 byte
2. Enkripsi DataTerdiri dari iterasi fungsi sederhana (Feistel Network)sebanyak 16 kali putaran.Setiap putaran terdiri daripermutasi kunci-dependentdan substitusi kunci dan data dependent. Semua operasi adalah penambahan(addition) dan XOR pada variabel 32-bit.Operasi tambahan lainnya hanyalah empat penelusuran tabel(table lookup) array berindeks untuk setiap putaran[3].

   Blowfish menggunakan sub-key besar yang harus dihitung sebelum enkripsi dan dekripsi data. Algoritma Blowfish menerapkan jaringan Feistel yang terdiri dari 16 putaran. Input adalah elemen 64-bit, X untuk alur algoritma enkripsi dengan metode Blowfish dijelaskan sebagai berikut[4]:

1. Inisialisasi P-array diikuti dengan empat S-boxes dengan string terdiri dari Pi hexadecimal.
2. P1 di-XOR dengan kunci 32-bit pertama, P2 di-XOR dengan kunci 32-bit kedua, proses diulang sampai semua P-array telah selesai di-XOR.
3. Algoritma lalu digunakan untuk mengenkripsi string kosong yang diisi dengan sub-key pada tahap 1 dan 2.
4. P1 dan P2 diganti dengan output tahap 3.
5. Enkripsi output tahap 3 dengan algoritma Blowfish menggunakan sub-key yang telah dimodifikasi.
6. Output dari tahap 5 digunakan untuk menggantikan P3 dan P4.
7. Proses akan terus diulang sampai semua P-array telah tergantikan, dilanjut dengan semua 4 S-boxes, dengan output yang terus berubah.

3. METODE PENELITIAN

Metode penelitian dalam pengembangan sistem kriptografi menggunakan algoritma Blowfish pada Minimarket ini menggunakan metode Waterfall Model yang meliputi :

1. Analisa Kebutuhan

   Dalam tahapan ini, penulis menentukan segala kebutuhan sistem dengan melihat data dan proses yang berjalan. Dalam tahapan ini juga penulis menentukan algoritma apa yang digunakan untuk melakukan enkrpsi data sehingga data yang telah disandikan terlindungi dengan baik.

2. Design Sistem

   Dalam tahapan ini penulis membuat design sistem kriptografi untuk data pada minimarket HappyMart. Pada tahapan ini juga penulis menentukan hirarki proses yang dilakukan sistem dari proses input data, enkrpsi data dan menyimpan data kedalam tabel.

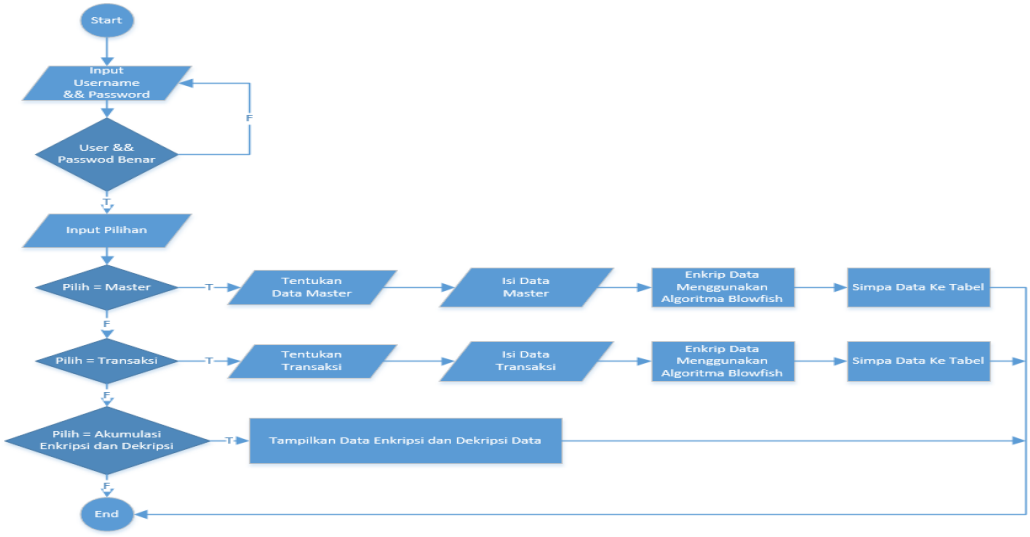
3. Pembuatan Sistem

   Berdasarkan analisa kebutuhan dan design sistem sebelumnya pada tahapan ini mulai dikerjakan pembuatan sistem yaitu mengimplementasikan design sistem kedalam bentuk coding sistem sehingga dapat dihasilkan sistem kriptografi pengamanan data pada minimarket HappyMart. Bahasa pemograman yang digunakan adalah berbasis WEB dengan menggunakan bahasa program PHP

4. Uji Coba dan Analisa Sistem
   Dalam tahapan ini dilakukan ujicoba sistem yang telah dibuat, apakah sudah sesuai dengan design dan kebutuhan sistem apabila belum dilakukan evaluasi kembali sampai dihasilkan sebuah sistem yang sesuai dengan kebutuhan.

4. HASIL DAN PEMBAHASAN

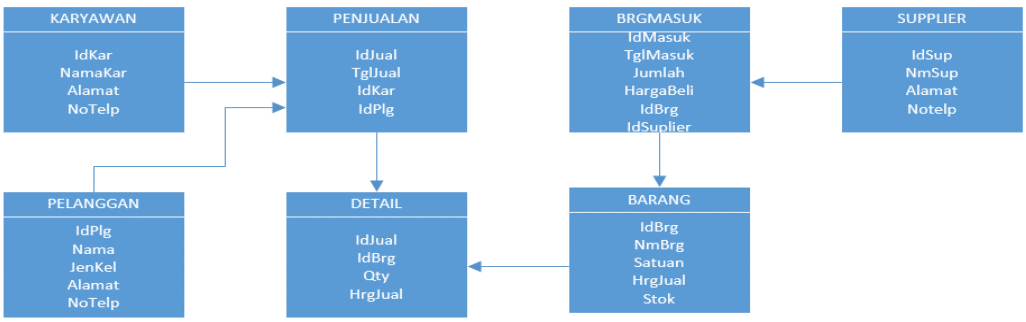
4.1. Algoritma Program Enkripsi dan Dekripsi Data HappyMart



Gambar 1. Algoritma Program

Pada gambar diatas, dijelaskan bagaimana hirarki proses pada sistem kriptografi database minimarket HappyMart barjalan. Dari hal yang pertama dilakukan yaitu user atau pengguna sistem harus melakukan otentikasi agar dapat masuk kedalam sistem kriptografi database minimarket HappyMart. Selanjutnya user diminta untuk memilih data master atau data transaksi, setelah memililh data master atau transaksi. Selanjutkan akan ditampilkan seluruh data master atau transaksi dan user tinggal menentukan data mana yang akan dlihat maupun ditambahakan. Data yang telah ditambahkan akan disimpan kedalam tabel dalam keadaan terenkripsi.

4.2. Struktur Tabel

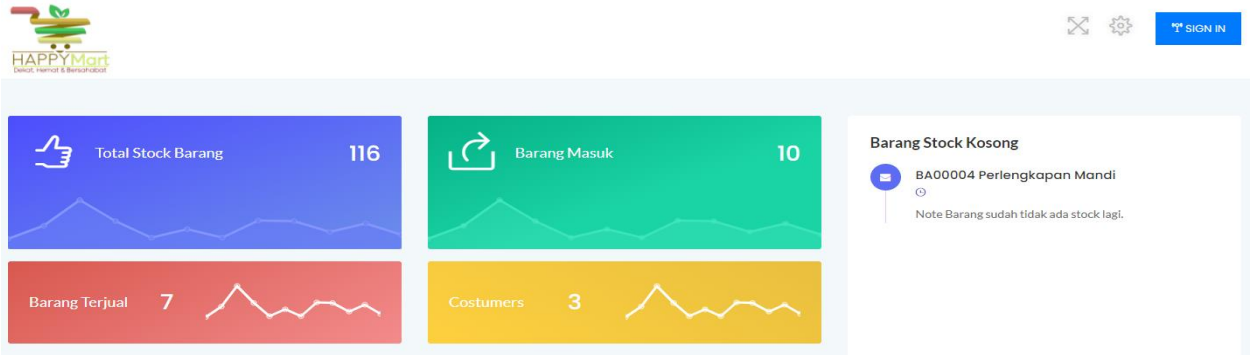


Gambar 2. Struktur Tabel

Pada gambar diatas, diperlihatkan bagaimana struktur tabel yang digunakan dalam sistem kriptografi database minimarket Happymart. Dapat juga dilihat bagaimana relasi atau hubungan antar entitas yang ada, serta informasi apa saja yang tersimpan kedalam tabel.

4.3 Sistem Enkripsi Data Minimarket

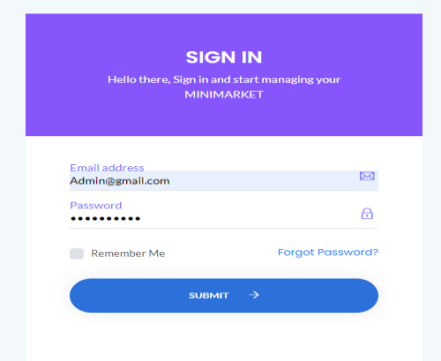
4.3.1 Halaman Home Sistem Enkripsi



Gambar 3. Halaman Home Sistem Enkripsi

Halaman Dashboard atau Home ini, merupakan halaman awal ketika sistem diakses. Pada halaman ini ditampilkan data dashboard berupa total stok barang yang ada, barang masuk atau pembelian barang, barang terjual, total customer serta jumlah barang dengan stok kosong.

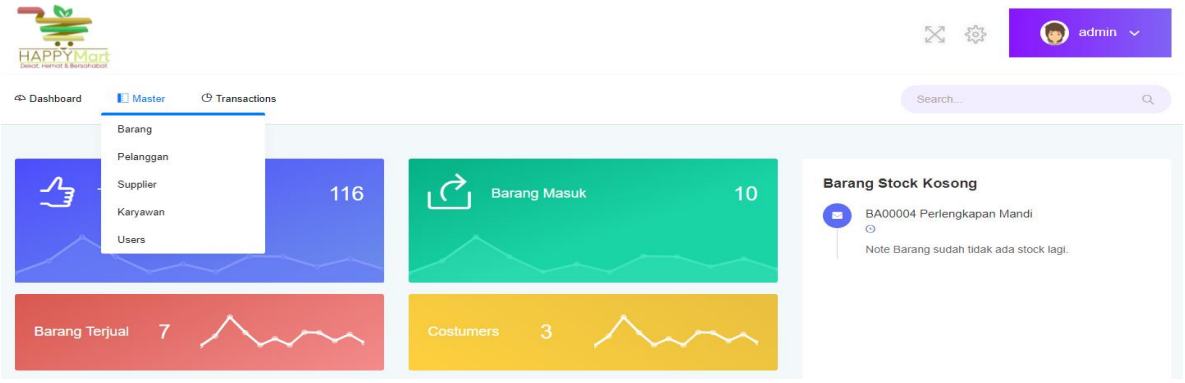
4.3.2 Halaman Login



Gambar 4. Halaman Login

Halaman Login, diperlukan untuk mengakses semua fitur sistem enkripsi data happy mart, untuk bisa masuk ke halaman menu utama diperlukan otentifikasi untuk mengidentifikasi user atau pengguna sistem.

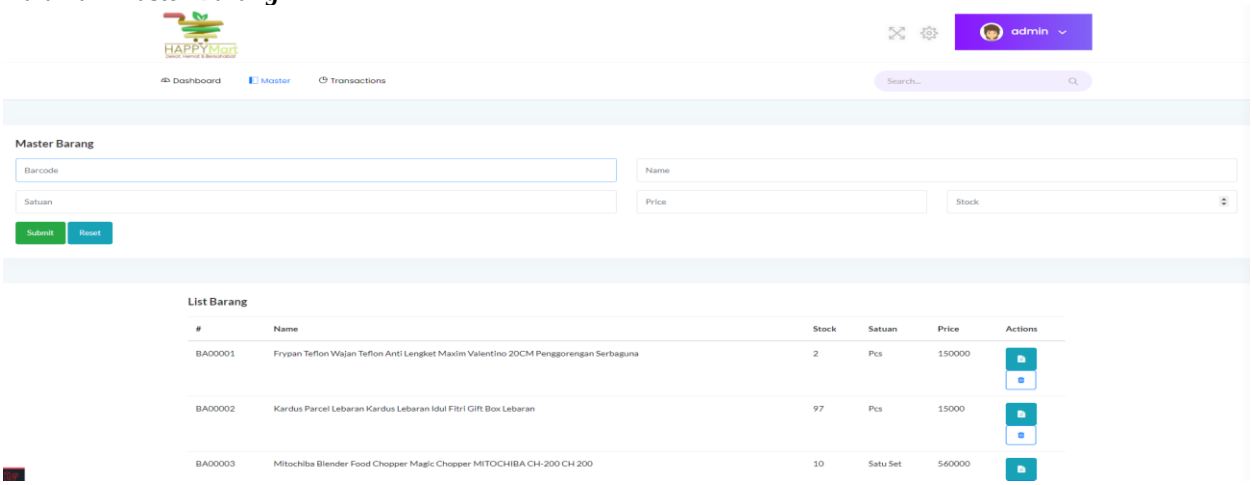
4.3.3 Halaman Menu Master



Gambar 5. Halaman Menu Master

Halaman Menu master, berisi data-data master. Berupa master barang, pelanggan, supplier, karyawan serta user. Semua data master ini pada saat disimpan kedalam database dalam keadaan dienkripsi. Akan tetapi ketika data ditampilkan dalam bentuk sistem informasi sudah dalam keaadaan didekripsi.

4.3.4 Halaman Master Barang



Gambar 6. Halaman Master Barang

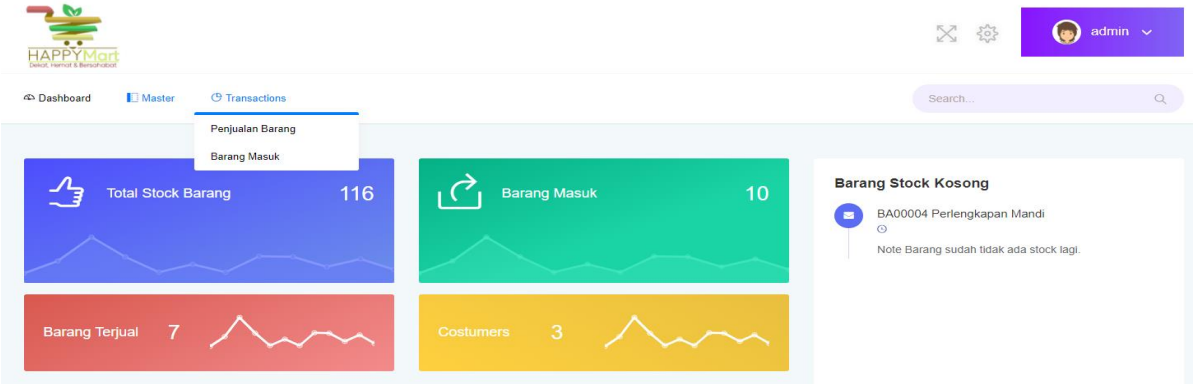
Halaman master barang, berisi tentang data-data barang hypermat. Pada halaman ini dapat dilakukan input data barang baru. Semua data barang yang diinput dilakukan enkripsi dengan menggunakan algoritma blowfish. Namun pada saat data ditampilkan Kembali sudah dalam keadaan didekripsi. Sehingga data yang disimpan dalam sistem database hanya bisa diakses dan dibaca informasinya melalu sistem enkripsi ini.

4.3.5 Halaman Hasil Enkripsi dan Dekripsi Data Barang

Gambar 7. Halaman Hasil Enkripsi dan Dekripsi Data Barang

Pada gambar diatas, baris pertama menunjukan data yang disimpan kedalam tabel barang berupa ciphertext atau penyandian data yang telah diinput sebelumnya menggunakan algoritma blowfish. data ciphertext ini melindungi data yang tersimpan kedalam tabel karena sudah berupa sandi sehingga tidak bisa dibaca langsung, memerlukan aplikasi sistem enkripsi untuk membaca datanya. Pada baris kedua merupakan hasil dekripsi data ciphertext, sehingga isi pesan data sandi atau ciphertext yang telah disimpan sebelumnya dapat dibaca informasi yang ada didalamnya karena sudah dilakukan dekripsi.

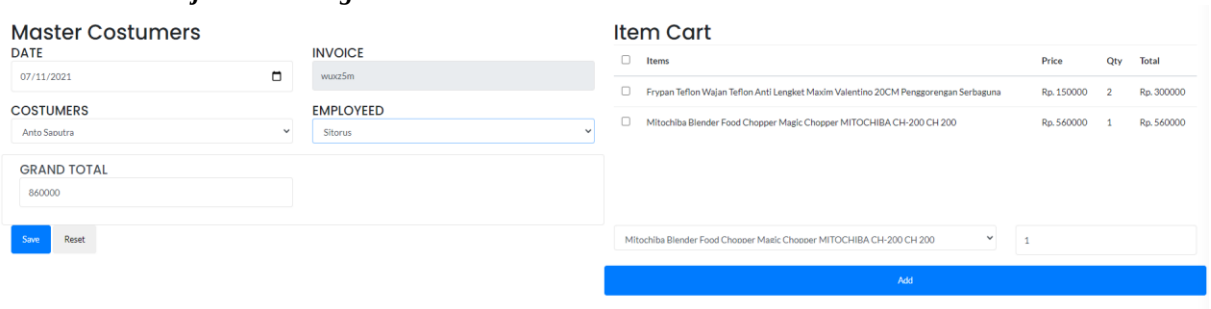
4.3.6 Halaman Menu Transaksi



Gambar 8. Halaman Menu Transaksi

Halaman transaksi, berisi tentang data transaki penjualan barang dan barang masuk pada HappyMart, data yang tersimpan dalam database sudah dalam keadaan terenkripsi menggunakan algoritma Blowfish. Sehingga data transaksi ini tidak bisa dibaca tampa menggunakan sistem enkripsi ini.

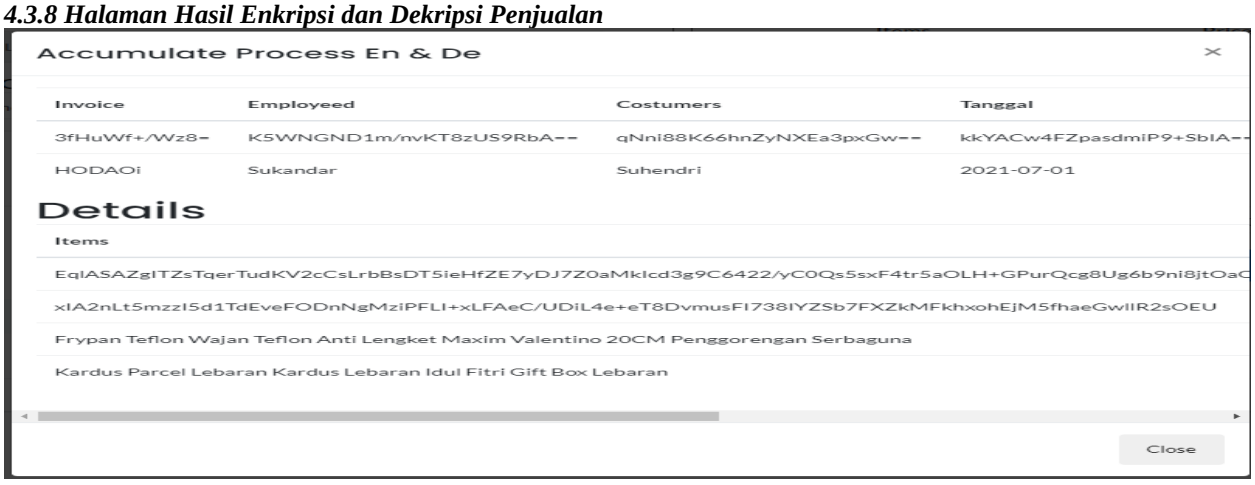
4.3.7 Halaman Penjualan Barang



Gambar 9. Halaman Penjualan Barang

Halaman ini berisi tentang data penjualan barang pada HappyMart, yang meliput data penjualan, data customer, data karyawan. Serta data barang yang di jual ke pelanggan. Data-data penjualan tersebut di enkripsi dengan algoritma BlowFish lalu di simpan kedalam tabel.

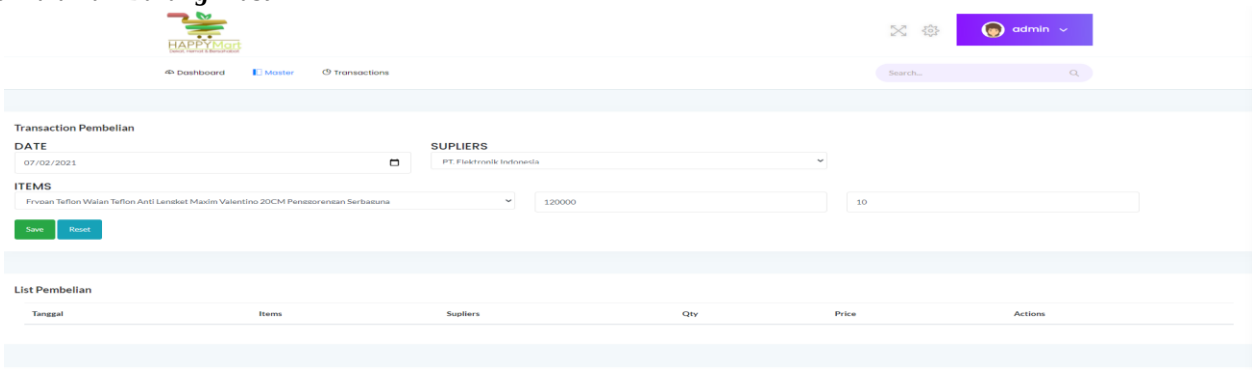
4.3.8 Halaman Hasil Enkripsi dan Dekripsi Penjualan



Gambar 10. Halaman Enkripsi dan Dekripsi Pengualan

Pada gambar diatas, ditampilkan penyandian data dan dekripsi data penjualan barang. Pada data penjualan barang ini terbagi atas dua bagian utama, yang pertama data invoice dan yang kedua adalah data detail barang. Pada bagian invoice dan detail barang data yang disimpan kedalam tabel berupa ciphertext atau penyandian data menggunakan algoritma blowfish. pada masing-masing bagian invoice dan detail barang juga ditampilkan hasil dekripsi yaitu proses pengembalian data sandi atau ciphertex kedalam bentuk plaintext atau mengembalikan data yang dienkrip sehingga data tersebut dapat dibaca kembali informasi yang ada didalamnya.

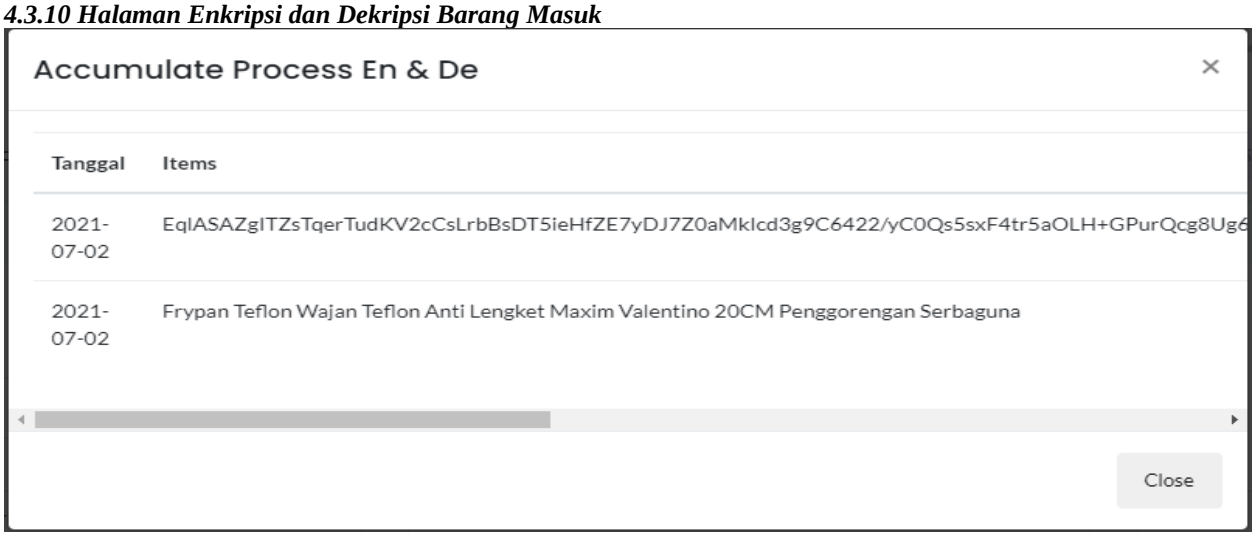
4.3.9 Halaman Barang Masuk



Gambar 11. Halaman Barang Masuk

Halaman barang masuk, berisi tentang barang-barang yang telah diberi dan diinput kedalam sistem. Data barang yang telah masuk akan disimpan kedalam sistem dengan menggunakan pengamanan data algoritma BlowFish. Sehingga data tersimpan dalam keadaan dienkripsi.

4.3.10 Halaman Enkripsi dan Dekripsi Barang Masuk



Gambar 12. Halaman Enkripsi dan Dekripsi Barang Masuk

Pada gambar diatas, menunjukan hasil proses enkripsi data dan dekripsi data barang masuk. Baris pertama menunjukan data ciphertext berupa sandi data yang tersimpan kedalam database mengunakan algoritma blowfish, sedangkan baris kedua menunjukan hasil penerjemahan ciphertext atau proses dekripsi mengembalikan data sandi ciphertext menjadi data semula berupa plaintext sehingga isi data dapat dibaca kembali.

5. KESIMPULAN

Berdasarkan analisa dan pembahasan yang telah disampaikan diatas, dapat ditarik beberapa kesimpulan diantaranya :

a. Penerapan algoritma untuk mengamankan data-data penting pada minimarket HappyMart dalam dilakukan dengan baik, dimana enkripsi data yaitu merubah plaintext menjadi ciphertext atau penyandian data dapat dilakukan berupa data atau informasi yang tersimpan kedalam tabel dalam keadaan terenkripsi.
b. Dengan adanya penyandian data pada data minimarket HappyMart memberikan proteksi tambahan terhadap data penting minimarket HappyMart. Sehingga tidak mudah untuk dicuri maupun dimanipulasi isi data tersebut.

DAFTAR PUSTAKA

[1] D. A. Meko, "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *J. Teknol. Terpadu*, vol. 4, no. 1, 2018.
[2] Y. P. Astuti, E. H. Rachmawanto, and C. A. Sari, "Optimasi Enkripsi Password Menggunakan Algoritma Blowfish," *Techno. Com*, vol. 15, no. 1, pp. 15–21, 2016.
[3] F. Kurniawan, "PERANCANGAN FORMULIR ELEKTRONIK DIENKRIPSI DENGAN METODE BLOWFISH PADA SISTEM PENDAFTARAN ONLINE (STUDI KASUS: SELEKSI MANDIRI UNIVERSITAS TANJUNGPURA)," *JUSTIN (Jurnal Sist. dan Teknol. Informasi)*, vol. 1, no. 1, pp. 44–49.
[4] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, and S. Srinjiwi, "Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan AlgoritmA RSA," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 6, no. 1, pp. 1–10, 2019.